**IT Applications, Unit 4**

**Ch 8, Security and Ethical Considerations**

**Disaster Recovery Strategies, p 514**

1. What is a disaster recovery plan?  
   A disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations, including computer, in the event of a disaster.

Preparing a disaster recovery plan:

1. List some considerations required in preparing a disaster recovery plan.  
   Conduct a risk assessment, identify recovery strategies and procedures, purchase products and services to support disaster recovery and test the system and maintain a plan.

There are four key parts to a disaster recovery plan:

1. Preparing an emergency plan
   1. What should an emergency plan contain?  
      names and contact details of people to notify, including management and emergency services  
      procedures to follow with the computer equipment, such as equipment shutdown or removal of files  
      evacuation procedures for employees, including removal of backup tapes or equipment  
      return procedures detailing who may re-enter the facility and under what circumstances and,  
      details of equipment supplies and insurance providers so that the information system can be rebuilt as quickly as possible.
2. Preparing a “backup” plan
   1. What does a backup plan involve?  
      covers the procedures that the company is to follow for using file backups to restore computer systems.
   2. List what the plan should include  
      the location of alternative sites and equipment in case the normal computer facility has been destroyed,  
      the location of backup data, supplies and equipment,  
      the personnel responsible for gathering backup resources and transporting them to the alternative computing facility and,  
      a schedule indicating the order and approximate time in which each application should be up and running.
3. Preparing a recovery plan
   1. What does a recovery plan involved?  
      includes specific procedures for restoring the full information processing capacity of the organisation.
   2. What are the things to consider when writing a recovery plan?  
      identification of mission-critical ICT services; these will have first priority when getting the system back online and,  
      use of a backup (or secondary) site for data-processing needs until the primary site has been recovered.
4. Test plan
   1. What is looked for in testing a disaster recovery strategy?  
      Typically, the test plan will contain information about simulating a variety of disasters and different recovery needs. When the simulation is carried out, each staff member carries out their assigned roles and procedures. If there are any problems with the disaster plan, they should be identified and corrected during testing. Ideally, a disaster simulation should be carried out without warning.

**Evaluating information-management strategies,** p 517

Elaborate on each of the following four criteria to consider in evaluating information-management strategies:

1. integrity of data  
   Data integrity depends on its accuracy, reliability and timeliness. Whether storing, transmitting or archiving data, you must be sure that its integrity is maintain. Otherwise, that data may not be accessible when needed.
2. security  
   If you have spent a great deal of money securing your data from threats, you want to be sure that the data security is effective. Audit trails and log files can alert you to any problems with logon or file access procedures. You need to be certain that the system is hacker-proof. If you can demonstrate that incidences of hacker attack have decreased or stopped altogether, this indicates that your security measures are working.
3. ease of retrieval  
   It can be extremely frustrating when it takes a long time to find a file that you need urgently. Naturally, you would expect that after you had stored or archived a file, it could be found and retrieved easily and quickly. Proper observance of folder and file-naming conventions will help staff to find documents. If the conventions are difficult to follow, however, files may be ‘lost’ or they may take more time to find. Using correct file extensions is import because it allows recognition by application software.
4. currency of files  
   Regular backups will help to ensure that the most recent versions of files are available if needed. If there has been a disaster and backup files are needed to restore the system, determine how much data has actually been lost and whether or not this is within the amount tolerated by the organisation.